

IN THE DISTRICT COURT OF THE UNITED STATES  
FOR THE DISTRICT OF SOUTH CAROLINA  
ANDERSON DIVISION

UNITED STATES OF AMERICA,	)	CIVIL ACTION NO.:
	)	
	)	
Plaintiff,	)	
	)	
vs.	)	
	)	
	)	
4,051.791686 USDT,	)	
	)	
Defendant <i>in Rem</i> .	)	

**UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM***

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

**NATURE OF THE ACTION**

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of 4,051.791686 USDT valued at approximately \$4,052.54 USD (“United States Dollars”), (“Defendant Funds”), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitute, or are traceable to:

- a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy of same in violation of 18 U.S.C. §§ 1343, 1349;
- b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;

- c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or
- d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7); and/or
- e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h); and/or
- f. property involved in money transactions in criminally derived property or attempted money transactions, in violation of 18 U.S.C. § 1957.

### **JURISDICTION AND VENUE**

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355.

This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

- (a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and
- (b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

### **THE DEFENDANT IN REM**

3. The Defendant Funds consist of 4,051.791686 USDT valued at approximately \$4,052.54 USD, obtained by agents with the United States Secret Service (“USSS”) during an investigation into a transnational criminal organization running an exploitation of elderly and social engineering scam. The funds were seized from a cryptocurrency custodial wallet under the control of Binance,

identified by account number ‘143466193’ (the “Suspect Wallet”) and under the name of MD Shahid Hussain (“Hussain”).

4. The USSS seized the 4,051.791686 USDT valued at approximately \$4,052.54 USD, for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of United States Secret Service.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately \$4,052.54.

### **KNOWN POTENTIAL CLAIMANTS**

6. The known individuals whose interests may be affected by this litigation are:

- a. MD Shahid Hussain, who may have an interest in the Defendant Funds because he was the named account holder of the account seized by USSS during this investigation.

### **BASIS FOR FORFEITURE**

7. Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

- a. USSS and local law enforcement agencies were investigating a transnational criminal organization running an exploitation of elderly and social engineering scam. In brief summary, investigating agents determined that a scamming group has been using social engineering to contact elderly individuals and convince them that their computers or

bank accounts are compromised. Once the scammers have engagement from the victim, they instruct them that their device is compromised and to work with tech support to resolve the issue. During this interaction, the victim is convinced to send the scammer their own funds. The victims then withdraw their funds in cash and take it to a BTC Automatic Teller Machine (“ATM”). From that ATM, the funds are sent to a cryptocurrency wallet address provided by the suspects.

b. As set forth below, the Subject Wallet was used by the scammers to receive and launder proceeds of the above-described scheme. Investigating agents believe that the Subject Wallet was created and used primarily for the purpose of laundering scheme proceeds.

c. Digital currency (also known as virtual currency or cryptocurrency) is generally defined as an electronic-source unit of value that can be used as a substitute for fiat currency (i.e. currency created and regulated by a government). Digital currencies exhibit properties similar to other currencies, but do not have a physical form, existing entirely on the internet. Digital currency is not issued by any government or bank (in contrast with fiat or conventional currencies) and is instead generated and controlled through computer software operating on a decentralized peer-to peer network, often referred to as the blockchain or public ledger. Digital currency is legal in the United States and accepted for legitimate financial transactions. However, digital currency is often used for conducting illegal transactions or for concealing or disguising the true nature, source, location, ownership or control of illegally obtained proceeds. Bitcoin (“BTC”) is one of the most

commonly used and well-known digital currencies. Ethereum (“ETH”) is another popular and commonly used digital currency.

d. A stablecoin is a digital currency whose market value is attached to or “pegged” to another stable asset. Differing from normal digital currencies, the value of stablecoins are pegged to assets such as fiat currencies like the United States Dollar (“USD”) or the Euro, or other types of assets like precious metals or other digital currencies. Stablecoins are thus used to mitigate the volatility in the price of digital currency by mimicking the value of a fiat currency, without actually converting digital currency into fiat. While there are various legitimate uses for stablecoins, they are popular with cyber-criminals who seek to hold digital currency proceeds of crime at a stable or near-fixed value without moving those funds into the legitimate financial system into a fiat currency such as USD. Some examples of stablecoins include:

- (1) Tether (USDT) was developed by Tether Limited Inc. and is designed to maintain its value at \$1.00 USD. USDT can utilize the existing ETH blockchain or the newer TRON (“TRX”) blockchain.

e. A digital currency exchange (an “exchange”) is a business that allows customers to trade digital currencies for other digital fiat currencies. An exchange can be a brick-and-mortar business, or strictly online business. Both brick and mortar and online exchanges accept a wide variety of digital currencies, and exchange them for fiat and traditional payment methods, other digital currencies, or transfers between digital currency owners. Most exchanges are located outside the boundaries of the United States in order to avoid

regulation and legal requirements, but some popular exchanges operate inside the jurisdiction of the United States. Binance is an example of a popular online exchange that is located outside of the United States but cooperates with and accepts legal process from American law enforcement agencies.

f. A wallet is a means of storing digital currency identified by unique electronic addresses that allows an individual to conduct transactions on the public ledger. To access a wallet on the public ledger an individual must use a public address (or “private key”). The public address can be analogized to an account number while the private address is similar to a password used to access that account. Even though the public address of those engaging in digital currency transactions are recorded on the public ledger, the true identities of the individuals or entities behind the public address are not recorded. If a real individual or entity is linked to a public address, however, it may be possible to determine what transactions were conducted by that individual or entity. Therefore, digital transactions are often described as “pseudonymous,” meaning they are partially anonymous. Most individuals are identified when they use a digital currency exchanger to make a transaction between digital currency and fiat, or through digital currency exchangers that voluntarily or through legal order, cooperate with law enforcement.

g. On or about April 18, 2024, M.S., a 77-year-old resident of Easley, S.C. received a pop up on her computer that she believed to be from her computer tech support, The Geek Squad. M.S. was instructed via this pop up to call a phone number to speak with a representative. In speaking with who she believed to be customer service, they apologized

for the issue and offered her a refund of \$399.

h. Upon entering the refund amount, the scammer indicated that she actually entered \$39,000.00 in the system and that the amount was deposited into her bank account. They became very concerned and told her that they could lose their job. They asked M.S. to go to the bank and withdraw \$15,000.00, what they said was the max possible amount daily and then send it back to them via Bitcoin.

i. M.S. traveled to her bank and withdrew \$15,000.00 in cash. She was then instructed to go to a Bitcoin ATM machine to send the funds to an account provided to her by the suspect. The suspect provided an address that the victim used to send the currency to. The cryptocurrency wallet address was 1PH7X7APUWCJVxcUm9AEL7SWB2CneonAGS (subject account). Once the victim sent the BTC to the wallet address provided, the scammer cut off all further communication. It was then that the victim checked her accounts and realized that the funds withdrawn from her account were not an over deposit from the scammers, but actually her own money.

j. On April 19, 2024, USSS Special Agent Lea reviewed the transaction history in Suspect Wallet 1 provided by the hosting exchange, Binance. On April 18, 2024, at 01:14 hours (UDT) 0.17851449 BTC was deposited into the wallet via transaction ID: 692bd1a7891b318a6e11f0772470e139bb6fb7b9cb98c3bfc6acabbd. Based on the experience of Special Agent Lea and the information from the victim, it is believed that this deposit was from M.S.

k. As discussed previously, Suspect Wallet 1 received numerous deposits from BTC ATM's that appear to be similar victims of scams as a result of 18 U.S.C. § 1343. The funds deposited are immediately converted to USDT and quickly withdrawn. In this instance, all previous funds had been withdrawn prior to the incoming deposit from M.S. Once those funds were deposited, a portion was withdrawn prior to the account being restricted. All funds remaining in the account are direct proceeds from the scam perpetrated on M.S.

l. Binance identified MD Shahid Hussain ("Hussain") as the account holder of Suspect Wallet 1. The wallet became active in May 2021. Since that time, Suspect Wallet 1 received 92 deposits totaling approximately \$588,807.00. Of which most incoming transactions were in BTC, which were immediately converted to USDT at a cost of transaction fees. This account received numerous transactions from US based Bitcoin ATM machines. These funds immediately being converted to USDT is indicative of illicit activity as an overt attempt to conceal the nature, source, and ownership of the funds.

m. Suspect Wallet 1 was used by the subjects to receive proceeds from victims of wire fraud and to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds obtained from the scam.

n. The Subject Wallet bore numerous red flags for a money laundering facilitation account, namely:

- (1) The Subject Wallet does not appear to hold digital currency for long, instead rapidly receiving and then retransmitting digital currency, and often in the form of stablecoins;
  - (2) The Subject Wallet does not appear to be engaged in any investment activity, as digital currency is rapidly moved in and out, and stablecoins are designed not to increase in value greater than the USD;
  - (3) While these amounts might be unsurprising in a commercial or business account, the Subject Wallet was opened as a personal account with no identified associated business;
  - (4) Public information searches for Hussain do not identify any legitimate businesses associated with Hussain which would justify a personal account receiving and sending these volumes of digital currency; and
  - (5) The transaction activity in the Subject Wallet appears consistent with a “layering” account in a money laundering scheme, where an account is used primarily to receive and convert criminal proceeds before transmitting the proceed on to another recipient, thus disguising the source of the proceeds and frustrating asset recovery and law enforcement.
- o. On April 22, 2024, Special Agent Lea obtained a federal seizure warrant for the contents of Binance Account 143466193 in the name of MD Shahid Hussain. Following service of this seizure warrant, Binance released the Defendant Funds consisting of 4,051.791686 to USSS.

8. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitute, or are traceable to:

- a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy of same in violation of 18 U.S.C. §§ 1343, 1349;
- b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i) and/or 1957;
- c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or
- d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7);
- e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h) and;
- f. property involved in money transactions in criminally derived property, in violation of 18 U.S.C. § 1957.

### **CONCLUSION**

9. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for

Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

Respectfully submitted,

ADAIR F. BOROUGHS  
UNITED STATES ATTORNEY

By: s/Carrie Fisher Sherard  
Carrie Fisher Sherard #10134  
Assistant United States Attorney  
55 Beattie Place, Suite 700  
Greenville, SC 29601  
(864) 282-2100

November 18, 2024